On Some Dynamical Systems in Finite Fields and Residue Rings

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

February 2, 2008

Abstract

We use character sums to confirm several recent conjectures of V. I. Arnold on the uniformity of distribution properties of a certain dynamical system in a finite field. On the other hand, we show that some conjectures are wrong. We also analyze several other conjectures of V. I. Arnold related to the orbit length of similar dynamical systems in residue rings and outline possible ways to prove them. We also show that some of them require further tuning.

1 Introduction

In a recent series of papers, V. I. Arnold [1, 2, 3, 4, 5, 6] has considered dynamical systems related to linear transformations in finite fields and residue rings and made a number of conjectures. We observe that the study of the length, distribution of element and other properties, of the orbits of such dynamical systems has a long and successful history, which dates back to early works of N. M. Korobov [46], H. Niederreiter [59, 60], A. G. Postnikov [66] and many other researchers. Here we show that some classical results immediately imply some of these conjectures. We also show that several other conjectures are not correct as they are stated in [1, 2, 3, 4, 5, 6] and need some adjustments.

For a prime p and a positive integer n, we denote by $\mathbb{F}_{p^n}$ the finite field of p^n elements (we refer to [52] for the background information on finite fields).

We fix a primitive root ϑ of $\mathbb{F}_{p^n}$ and recall that we also have $\mathbb{F}_{p^n} \cong \mathbb{F}_p[\vartheta]$. In particular, $\mathbb{F}_{p^n}$ can be considered as an n-dimensional vector space over $\mathbb{F}_p$, where with each element $\alpha \in \mathbb{F}_{p^n}$ one can associate the coordinate vector $\mathbf{a} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_p^n$ from the expansion

$$\alpha = \sum_{j=0}^{n-1} a_j \vartheta^{j-1}.$$

Accordingly, V. I. Arnold [4] suggests to study the sequence of vectors $\mathbf{a}_m = (a_{0,m}, \ldots, a_{n-1,m}) \in \mathbb{F}_p^n$ corresponding to the powers

$$\vartheta^m = \sum_{j=0}^{n-1} a_{j,m} \vartheta^{j-1}. \tag{1}$$

Clearly, assuming that $\mathbb{F}_p$ is represented by the elements of the set $\{0, 1, \ldots, p-1\}$, one can view the points

$$\frac{1}{p}\mathbf{a}_m, \qquad m = 1, \ldots, M, \tag{2}$$

as M points of an n-dimensional unit cube $[0,1]^n$. For $M = p^n - 1$ these points form a regular cubic lattice (with only one missing point $(0, \ldots, 0)$). It has also been conjectured by V. I. Arnold [4] that in fact even the first $M < p^n - 1$ powers already form a rather uniformly distributed point set. Namely, given a region $\Omega \in [0,1]^n$ with smooth boundary, we denote by $N_\vartheta(M, \Omega)$ the number of points (2) which belong to Ω. The conjecture of Section 2.A of [4] asserts that

$$N_\vartheta(M, \Omega) = M \operatorname{vol} \Omega + o(M) \tag{3}$$

provided that $M \sim \mu p^n$ for some fixed $\mu > 0$ (and $p \to \infty$).

We start with an observation that using classical bounds of incomplete exponential sums with exponential functions, see [45, 46, 52], and some standard tools from the theory of uniform distribution, see Section 2.4, one can derive the following improved version of the conjecture (3):

$$N_\vartheta(M, \Omega) = M \operatorname{vol} \Omega + O\left(M^{1-1/n} p^{1/2n} (\log p)^{1+1/n}\right), \tag{4}$$

which is nontrivial whenever $M/p^{1/2}(\log p)^{n+1} \to \infty$. In fact, using some results of H. Niederreiter [59, 60] one can easily extend the above result in several directions.

In fact, using the results of J. Bourgain and M.-C. Chang [13], which in turn generalize several recently emerged results of J. Bourgain, A. A. Glibichuk and S. V. Konyagin [14, 15], one can also study the distribution in intervals of the set (2) for extremely small values of M. For example, see [16] for more details and a version of the bound (4) which is nontrivial provided that $M \geq p^{\varepsilon}$ for any fixed $\varepsilon > 0$ and sufficiently large p. The bound of the error term in [16] is not completely explicit, so for large values of M the bound (4) is better than that of [16].

Moreover, for $n = 1$, that is, for prime fields, using bounds of exponential sums from [9, 34, 36], one can obtain nontrivial results for even smaller intervals, which however holds only for almost all primes p (rather than for all p).

Furthermore, motivated by the results of [11, 32], we consider the distribution of vectors $\mathbf{a}_m$ where instead of an initial segment $[1, M]$, m runs through the values of a polynomial. Unfortunately, we are not able to treat arbitrary polynomials with integer coefficients for every primitive root ϑ but rather obtain a result which holds for almost all primitive roots. However, in the case of monomials, employing the bound of exponential sums with the sequence ϑ^{m^k}, $m = 1, 2, \ldots$, from [27], we obtain a nontrivial estimate for every primitive root ϑ.

V. I. Arnold [1, 3, 5, 6] also describes similar dynamical systems in the residue ring $\mathbb{Z}_\ell$ modulo ℓ and makes several conjectures about the length of the orbits. More specifically, given an integer $g \geq 2$ with $\gcd(g, \ell) = 1$, V. I. Arnold [1, 3, 5, 6] suggests to consider the dynamical properties of the residues $g^m \pmod{\ell}$.

We recall that the *Carmichael function* $\lambda(\ell)$ is defined for all $\ell \geq 1$ as the largest order of any element in the multiplicative group $\mathbb{Z}_\ell^*$. More explicitly, for any prime power p^ν, one has

$$\lambda(p^\nu) = \begin{cases} p^{\nu-1}(p-1) & \text{if } p \geq 3 \text{ or } \nu \leq 2, \\ 2^{\nu-2} & \text{if } p = 2 \text{ and } \nu \geq 3, \end{cases}$$

and for an arbitrary integer $\ell \geq 2$,

$$\lambda(\ell) = \operatorname{lcm}\left(\lambda(p_1^{\nu_1}), \ldots, \lambda(p_s^{\nu_s})\right),$$

where $\ell = p_1^{\nu_1} \ldots p_s^{\nu_s}$ is the prime factorization of ℓ. Clearly, $\lambda(1) = 1$. We also let $\varphi(\ell)$ denote the *Euler function*, which is defined as usual by

$$\varphi(\ell) = \#\mathbb{Z}_\ell^* = \prod_{j=1}^{s} p_j^{\nu-1}(p_j - 1),$$

with $\varphi(1) = 1$. Finally, for a an integer g with $\gcd(g, \ell) = 1$, we denote by $t_g(\ell)$ the multiplicative order of g modulo ℓ. Clearly, we have the divisibilities

$$t_g(\ell) \mid \lambda(\ell) \mid \varphi(\ell).$$

Several conjectures of [1, 3, 5, 6] can be reformulated as various statements about the relative size of $t_g(\ell)$, $\lambda(\ell)$ and $\varphi(\ell)$, on average and individually. We discuss these conjectures and show that some of them are already known in the literature, while some can be proved to be wrong. It is suggested in Section 1 of [5] that for $g = 2$ the average multiplicative order

$$T_g(L) = \frac{1}{L} \sum_{\substack{\ell=1 \\ \gcd(g,\ell)=1}}^{L} t_g(\ell)$$

grows like

$$T_g(L) \sim c(g) \frac{L}{\log L} \tag{5}$$

for some constant $c(g) > 0$ depending only on g (we note that in [5] it is made explicit only for $g = 2$).

We show that the classical result of Hooley [42] on *Artin's conjecture*, implies, under the *Extended Riemann Hypothesis*, that the conjecture (5) is wrong and in fact

$$T_g(L) \geq \frac{L}{\log L} \exp\left(C(g)(\log\log\log L)^{3/2}\right).$$

for some constant $C(g) > 0$ depending only on g. Furthermore, we believe that in fact $T_g(L)$ grows even faster. It is possible that the method of proof of Theorems 1 and 2 in [8], which in turn is an extension of the method of [57] (see also [25]), together with the result of Hooley [42], can be used to derive that, under the Extended Riemann Hypothesis,

$$T_g(L) \geq \frac{L}{\log L} \exp\left((\log\log\log L)^{2+o(1)}\right). \tag{6}$$

For the upper bound it is probably natural to assume that

$$T_g(L) = o\left(\frac{1}{L}\sum_{\ell=1}^{L} \lambda(\ell)\right). \tag{7}$$

Note the sum on the right hand side of (7) has been estimated by P. Erdős, C. Pomerance and E. Schmutz [24].

Finally, we give a guide to the literature concerning results and methods which can probably be of great use for the theory of algebraic dynamical systems over finite fields and rings.

It is very well known that there are close ties between number-theory and dynamical systems. For example, one can associate dynamical systems with continued fractions, various number systems, the $3x+1$ transformation and other number-theoretic constructions. A wealth of very interesting results can be found in the literature.

However, we would like to use this paper as an opportunity to attract more attention of the dynamical system community to a great variety of already existing number theoretic results and techniques which can be of great significance for studying various algebraic dynamical systems. In particular, these include, but are not limited too, bounds on various exponential sums, periods of various sequences and average values of associated arithmetic functions, For this very purpose we do not try to formulate and prove our results in their full generality but rather limit ourselves to the most interesting and illuminating special cases. We however indicate possible extensions of our results and directions for further research.

Although exponential sums have been used for this purpose, see the work of M. Degli Esposti and S. Isola [18] and of P. Kurlberg and Z. Rudnick [48], their full potential seems to be not fully used in the dynamical system theory. We would like to stress that all such applications follow the same pattern:

$$\boxed{\text{bounds of exponential sums}}$$
$$\Downarrow$$
$$\boxed{\text{distribution in aligned boxes}}$$
$$\Downarrow$$
$$\boxed{\text{distribution in arbitrary regions with smooth boundary}}$$
$$\Downarrow$$
$$\boxed{\text{ergodic properties of the corresponding dynamical system}}$$

The link between exponential sums and the distribution in aligned boxes is provided by the Koksma–Szüsz inequality, see Theorem 1.21 of [19].

The link between the distribution in aligned boxes and arbitrary regions is given by the results of H. Niederreiter and J. M. Wills [64] and their more recent refinement of M. Laczkovich [49].

Surprisingly enough, the essentially tautological link between the distribution in arbitrary regions and ergodic properties has never been exploited in a systematic way, although it definitely deserves much more attention which we hope to attract with this paper.

2 Dynamical systems in finite fields

2.1 Preliminaries

Here we show how well known bounds of exponential sums can be used to derive various results about the orbits of $\vartheta^{f(m)}$, with a polynomial $f(X) \in \mathbb{Z}[X]$.

Throughout this section, any implied constants in the symbols O may depend on n and Ω (and occasionally, where obvious, on an integer parameter k).

As we have mentioned, the results of in this section can be extended in several directions.

2.2 Background on finite fields

Let $\omega_0, \ldots, \omega_{n-1}$ be a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ which is dual to the basis $1, \vartheta, \ldots, \vartheta^{n-1}$. That is,

$$\mathrm{Tr}\,\left(\omega_i \vartheta^j\right) = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{otherwise}; \end{cases} \qquad 0 \le i, j \le n-1,$$

where

$$\mathrm{Tr}\,(\alpha) = \sum_{k=0}^{n-1} \alpha^{p^k}$$

is the trace of $\alpha \in \mathbb{F}_{p^n}$ in $\mathbb{F}_p$.

Therefore, from (1) we derive

$$a_{j,m} = \mathrm{Tr}\,\left(\omega_j \vartheta^m\right) \tag{8}$$

for every $j = 0, \dots n-1$ and $m = 1, 2, \dots$.

It is also useful to recall that there are $\varphi(p^n - 1)$ primitive roots of $\mathbb{F}_{p^n}$.

2.3 Background on exponential sums

Let us denote $\mathbf{e}_p(z) = \exp(2\pi i z/p)$. Then for every $\gamma \in \mathbb{F}_{p^n}$ the function $\alpha \mapsto \mathbf{e}_p(\gamma \mathrm{Tr}(\alpha))$ is an additive character of $\mathbb{F}_{p^n}$.

For example, it follows immediately from a combination of Theorem 8.24 and Theorem 8.81 of [52] (see also [45, 46] and the references therein), that for any $M \le p^n - 2$ the following bound holds

$$\max_{\gamma \in \mathbb{F}_{p^n}^*} \left| \sum_{m=1}^{M} \mathbf{e}_p \left(\mathrm{Tr} \left(\gamma \vartheta^m \right) \right) \right| = O(p^{n/2} \log p). \tag{9}$$

The following estimate is a special case of a more general result of [35]. We remark that in [35] it is shown only in the case $n = 1$ but the proof extends to arbitrary fields without any changes.

Lemma 2.1. *For any primitive root $\vartheta \in \mathbb{F}_{p^n}$, any two subsets $\mathcal{X}, \mathcal{Y} \in \mathbb{Z}_{p^n-1}$ and any function $\psi(y)$ with*

$$\max_{y \in \mathcal{Y}} |\psi(y)| \le \Psi,$$

the following bound holds

$$\max_{\gamma \in \mathbb{F}_{p^n}^*} \sum_{x \in \mathcal{X}} \left| \sum_{y \in \mathcal{Y}} \psi(y) \mathbf{e}_p \left(\mathrm{Tr} \left(\gamma \vartheta^{xy} \right) \right) \right| = O\left(\Psi p^{9n/8 + o(1)} \left(\# \mathcal{Y} \right)^{3/4} \right).$$

We know recall the bound of exponential sums with ϑ^{m^k} from [27] which we use in the proof of Theorem 2.7. More precisely, we use Theorem 6 (for $k = 2$) and Theorem 7 (for $k \ge 3$) of [27] (we remark that in [27] these results are proven only for $n = 1$ but the general case can be obtained by a simple typographical change of p to p^n).

Let us define

$$\rho(k) = \begin{cases} \dfrac{1}{8}, & \text{if } k = 2; \\ \\ \dfrac{\lceil k/2 \rceil - 1}{2k \lceil k/2 \rceil + 2}, & \text{if } k \ge 3. \end{cases} \tag{10}$$

Lemma 2.2. *For any primitive root $\vartheta \in \mathbb{F}_{p^n}$, the following bound holds*

$$\max_{\gamma \in \mathbb{F}_{p^n}^*} \left| \sum_{m=1}^{p^n-1} \mathbf{e}_p \left(\mathrm{Tr} \left(\gamma \vartheta^{m^k} \right) \right) \right| \le p^{(1-\rho(k))n+o(1)}.$$

2.4 Background on discrepancies

For a finite set $\mathcal{U} \subseteq [0,1]^n$ and domain $\Omega \subseteq [0,1]^n$, we define the Ω-*discrepancy*

$$\Delta(\mathcal{U}, \Omega) = \left| \frac{\#\{\mathbf{u} \in \mathcal{U} \cap \Omega\}}{\#\mathcal{U}} - \mathrm{vol}\, \Omega \right|,$$

and the *box discrepancy* of $\mathcal{U}$,

$$D(\mathcal{U}) = \sup_{\mathbf{B} \subseteq [0,1]^n} \Delta(\mathcal{U}, \mathbf{B}),$$

where the supremum is taken over all boxes $\mathbf{B} = [\alpha_1, \beta_1] \times \ldots \times [\alpha_k, \beta_k]$.

We define the distance between a vector $\mathbf{u} \in [0,1]^n$ and a set $\Gamma \subseteq [0,1]^n$ by

$$\mathrm{dist}(\mathbf{u}, \Gamma) = \inf_{\mathbf{w} \in \Gamma} \|\mathbf{u} - \mathbf{w}\|$$

where $\|\mathbf{v}\|$ denotes the Euclidean norm of $\mathbf{v} \in \mathbb{R}^n$. Given $\varepsilon > 0$ and a domain $\Omega \subseteq [0,1]^n$ we define the sets

$$\Omega_\varepsilon^+ = \{\mathbf{u} \in [0,1]^n \backslash \Omega \mid \mathrm{dist}(\mathbf{u}, \Omega) < \varepsilon\}$$

and

$$\Omega_\varepsilon^- = \{\mathbf{u} \in \Omega \mid \mathrm{dist}(\mathbf{u}, [0,1]^n \backslash \Omega) < \varepsilon\}.$$

Let $b(\varepsilon)$ be any increasing function defined for $\varepsilon > 0$ and such that $\lim_{\varepsilon \to 0} b(\varepsilon) = 0$. Following [49, 64], we define the class $\mathcal{M}_b$ of domains $\Omega \subseteq [0,1]^n$ for which

$$\mathrm{vol}\, \Omega_\varepsilon^+ \le b(\varepsilon) \qquad \text{and} \qquad \mathrm{vol}\, \Omega_\varepsilon^- \le b(\varepsilon).$$

As special case of a result of H. Weyl [69] implies that for domains Ω with a piecewise smooth boundary, one can take $b(\varepsilon) = O(\varepsilon)$.

Lemma 2.3. *For any domain $\Omega \subseteq [0,1]^n$ with a piecewise smooth boundary*

$$\mathrm{vol}\, \Omega_\varepsilon^\pm = O(\varepsilon)$$

A relation between $D(\mathcal{U})$ and $\Delta(\mathcal{U},\Omega)$ for $\Omega \in \mathcal{M}_b$ is given by the following inequality from [49] (see also [64]).

Lemma 2.4. *For any domain $\Omega \in \mathcal{M}_b$, we have*

$$\Delta(\mathcal{U},\Omega) = O\left(b\left(n^{1/2} D(\mathcal{U})^{1/n}\right)\right).$$

The *Koksma–Szüsz inequality*, see Theorem 1.21 of [19], provides an important link between box discrepancy and exponential sums:

Lemma 2.5. *For any integer $L > 1$, and a set $\mathcal{U} \subseteq [0,1]^n$ of M points, one has*

$$D(\mathcal{U}) = O\left(\frac{1}{L} + \frac{1}{M} \sum_{\substack{\mathbf{c}=(c_0,\ldots,c_{n-1})\in\mathbb{Z}^n\setminus\{\mathbf{0}\}\\ |c_j|\le L\ j=0,\ldots,n-1}} \prod_{j=0}^{n-1} \frac{1}{(1+|c_j|)} \left|\sum_{\mathbf{u}\in\mathcal{U}} \exp\left(2\pi i \mathbf{c}\cdot\mathbf{u}\right)\right|\right),$$

where

$$\mathbf{c}\cdot\mathbf{u} = \sum_{j=0}^{n-1} c_j u_j$$

denotes the inner product of $\mathbf{c} = (c_0,\ldots,c_{n-1})$ and $\mathbf{u} = (u_0,\ldots,u_{n-1})$.

To estimate the box discrepancy of the set (2) we apply Lemma 2.5 with $L = (p-1)/2$. By (8) we see that the corresponding exponential sums takes shape

$$\sum_{m=1}^{M} \mathbf{e}_p\left(\sum_{j=0}^{n-1} c_j \mathrm{Tr}\left(\omega_j \vartheta^m\right)\right) = \sum_{m=1}^{M} \mathbf{e}_p\left(\mathrm{Tr}\left(\gamma\vartheta^m\right)\right)$$

where $\gamma = c_0\omega_0 + \ldots + c_{n-1}\omega_{n-1} \in \mathbb{F}_{p^n}^*$.

Applying the bound (9) together with Lemma 2.5, we see that the box discrepancy of the set (2) is $O\left(M^{-1}p^{n/2}(\log p)^{n+1}\right)$, see also [59, 60] and references therein for several more general results. Now the bound (4) follows directly from Lemmas 2.3 and 2.4.

2.5 Distribution of points in orbits

.

For an polynomial $f(X) \in \mathbb{Z}[X]$ and a given region $\Omega \in [0,1]^n$ with smooth boundary, we denote by $N_\vartheta(f; M, \Omega)$ the number of points

$$\frac{1}{p}\mathbf{a}_{f(m)}, \qquad m = 1, \ldots, M, \tag{11}$$

which belong to Ω.

Theorem 2.6. *Let $f(X) \in \mathbb{Z}[X]$ be a fixed nonconstant polynomial and let Θ be the set of all $\varphi(p^n - 1)$ primitive roots of $\mathbb{F}_{p^n}$. For any positive integer $M \le p^n - 1$ and any region $\Omega \in [0,1]^n$ with piecewise smooth boundary, we have*

$$\frac{1}{\varphi(p^n-1)} \sum_{\vartheta \in \Theta} |N_\vartheta(f; M, \Omega) - M \mathrm{vol}\, \Omega| \le M^{1-1/4n} p^{1/8+o(1)}.$$

Proof. To estimate the box discrepancy of the set (11) we apply Lemma 2.5 with $L = (p-1)/2$. As in Section 2.4, by (8) we see that the corresponding exponential sums takes shape

$$\sum_{m=1}^{M} \mathbf{e}_p \left(\sum_{j=0}^{n-1} c_j \mathrm{Tr}\, \left(\omega_j \vartheta^{f(m)}\right) \right) = \sum_{m=1}^{M} \mathbf{e}_p \left(\mathrm{Tr}\, \left(\gamma \vartheta^{f(m)}\right)\right)$$

where $\gamma = c_0\omega_0 + \ldots + c_{n-1}\omega_{n-1} \in \mathbb{F}_{p^n}^*$. Applying Lemma 2.5, we see that the box discrepancy $D_\vartheta(f; M)$ of the set (2) satisfies

$$\sum_{\vartheta \in \Theta} D_\vartheta(f; M) = O\left(\frac{1}{p} + \frac{(\log p)^n}{M} \max_{\gamma \in \mathbb{F}_{p^n}^*} \sum_{\vartheta \in \Theta} \left| \sum_{m=1}^{M} \mathbf{e}_p \left(\mathrm{Tr}\, (\gamma \vartheta^{f(m)})\right) \right| \right).$$

Let $\mathcal{X}$ be the set of all elements of $\mathbb{Z}_{p^n-1}$ which are relatively prime to $p^n - 1$. Fix an arbitrary primitive root $\vartheta_0 \in \mathbb{F}_{p^n}$. Then $\Theta = \{\vartheta_0^x \mid x \in \mathcal{X}\}$.

We denote by $\mathcal{Y}$ the value set $\mathcal{Y} = \{f(m) \pmod{p^n - 1} \mid m = 1, \ldots, M\}$ and by $\psi(y)$ the multiplicity of $y \in \mathcal{Y}$ (that is, the number of $m = 1, \ldots, M$ with $y \equiv f(m) \pmod{p^n - 1}$). In particular, $\#\mathcal{Y} \le M$ and by the famous Nagell–Ore theorem (see [43] for its strongest known form) we have

$$\Psi = \max_{y \in \mathcal{Y}} |\psi(y)| = p^{o(1)}.$$

We derive from Lemma 2.1 that

$$\max_{\gamma \in \mathbb{F}_{p^n}^*} \sum_{\vartheta \in \Theta} \left| \sum_{m=1}^{M} \mathbf{e}_p \left(\mathrm{Tr}\, (\gamma \vartheta^{f(m)})\right) \right| \le p^{9n/8+o(1)} M^{3/4},$$

which implies the bound

$$\sum_{\vartheta\in\Theta} D_\vartheta(f;M) \le p^{9n/8+o(1)} M^{-1/4}. \qquad (12)$$

Now, since Ω has a piecewise smooth boundary, from Lemmas 2.3 and 2.4 and the Hölder inequality, we derive

$$\begin{aligned}\sum_{\vartheta\in\Theta} |N_\vartheta(f;M,\Omega) - M\mathrm{vol}\,\Omega| &= O\left(M\sum_{\vartheta\in\Theta} D_\vartheta(f;M)^{1/n}\right)\\ &= O\left(M\left(\varphi(p^n-1)^{n-1}\sum_{\vartheta\in\Theta} D_\vartheta(f;M)\right)^{1/n}\right)\\ &= O\left(M\varphi(p^n-1)^{1-1/n}\left(\sum_{\vartheta\in\Theta} D_\vartheta(f;M)\right)^{1/n}\right).\end{aligned}$$

Since $k/\varphi(k) = O(\log\log k)$ for every integer k, see Theorem 328 of [40], from (12) we derive the desired estimate. □

For example, we see from Theorem 2.6 that for every fixed ε and $M \ge p^{n/2+\varepsilon}$, for almost all primitive roots of $\vartheta \in \mathbb{F}_{p^n}$, we have $N_\vartheta(f;M,\Omega) \sim M\mathrm{vol}\,\Omega$ for every region $\Omega \in [0,1]^n$ with smooth boundary.

For primes p such that p^n-1 has a certain prescribed arithmetic structure M.-C. Chang [16] obtained nontrivial results which hold for all primitive roots, rather than on average. Such primes are rather sparse but one can show that there are infinitely many of them.

Now, for an integer $k \ge 1$ and a given region $\Omega \in [0,1]^n$ with smooth boundary, we denote by $N_{\vartheta,k}(\Omega)$ the number of points

$$\frac{1}{p}\mathbf{a}_{m^k}, \qquad m = 1,\ldots,p^n-1, \qquad (13)$$

which belong to Ω.

As before, we define $\rho(k)$ by (10).

Theorem 2.7. *For any primitive root $\vartheta \in \mathbb{F}_{p^n}$ and any region $\Omega \in [0,1]^n$ with piecewise smooth boundary, we have*

$$N_{\vartheta,k}(\Omega) = p^n\mathrm{vol}\,\Omega + O\left(p^{n-\rho(k)+o(1)}\right).$$

Proof. Arguing as in the proof of Theorem 2.6, and using Lemma 2.2 instead of Lemma 2.1, we easily deduce that the box discrepancy of the set (13) can be estimated as $O\left(p^{-\rho(k)n+o(1)}\right)$. Now applying Lemmas 2.3 and 2.4 we conclude the proof. $\square$

We remark that similar results can be obtained in a more general situation (for example without the request that ϑ is a primitive root). We however follow the settings which exactly correspond to those of Section 2.A of [4].

2.6 Some other conjectures and open questions

In Section 2.B of [4] a conjecture is made which essentially means that the consecutive values ϑ^m, ϑ^{m+1} are independently distributed. It is easy to see that this is incorrect. For example, if $n = 1$ and $\vartheta = 2$ is primitive root modulo p (see [42]) then if $\vartheta^m \in (p/4, p/2)$ then $\vartheta^m \in (p/2, p)$, which happens for about $p/4$ values of $m = 1, \ldots, p-1$, while a conjecture given in Section 2.B of [4] predicts that this should happen for about $3p/16$ values of m.

Sections 2.C and 2.D of [4] contain a number of interesting questions about the geometric properties of the set of points (2). We remark that the bound $O\left(M^{-1}p^{n/2}(\log p)^{n+1}\right)$ on the box discrepancy of (2) obtained in Section 2.4, immediately implies that any aligned cube $[\alpha, \beta]^n$ inside of the unit cube $[0, 1]^n$ with the side length $\beta - \alpha > CM^{-1/n}p^{1/2}(\log p)^{1+1/n}$, for an appropriate constant $C > 0$, contains at least one point (2). This immediately implies upper bounds of the same order on the largest distance between the points (2) and on the largest radius of a ball inside of $[\alpha, \beta]^n$ which does not contain any points (2). Moreover, using some standard modifications, see [17], one can drop the logarithmic factor from these bounds.

3 Dynamical systems in residue rings

3.1 Preliminaries

Given an integer $g \geq 2$ with $\gcd(g, \ell)$, V. I. Arnold [1, 3, 5, 6] suggests to consider the dynamical properties of iterations of the map $x \mapsto gx$ in the residue ring $\mathbb{Z}_\ell$ (which is equivalent to studying the residues $g^m \pmod{\ell}$, in particular to studying the multiplicative order $t_g(\ell)$). In particular, in the

papers [1, 3, 5, 6] a number of suggestions have been made about the average orbit length of this and several similar dynamical systems.

We remark that indeed if the orbit length is sufficiently large then, following the standard scheme, one can derive some analogues of (4) from well known bounds of exponential sums [45, 46, 52, 59, 60].

Here we provide a brief guide to the literature and demonstrate that many existing techniques are suitable for studying these questions and in fact imply that some conjectures of [1, 3, 5, 6], based on numerical calculations, need some further adjustments.

Throughout this section, the implied constants in the Landau symbol 'O' and in the Vinogradov symbols '$\ll$' and '$\gg$' may occasionally, where obvious, depend on g, and are absolute otherwise (we recall that $U \ll V$ and $V \gg U$ are both equivalent to the inequality $U = O(V)$).

3.2 Analytic number theory background

Let $\pi_g(x)$ denotes the number of primes $p \le x$, such that g is a primitive root modulo p.

We recall the following celebrated result of Hooley [42]:

Lemma 3.1. *Under the Extended Riemann Hypothesis, for every integer g which is not a perfect square, there exists a constant $A(g) > 0$ such that*

$$\pi_g(x) \sim A(g) \frac{x}{\log x}.$$

Let $\pi(x; k, a)$ denote the number of primes $p \le x$ with $p \equiv a \pmod k$. We need the following relaxed version of the *Brun–Titchmarsh* theorem, see Theorem 3.7 in Chapter 3 of [39].

Lemma 3.2. *For any integers $k, a \ge 1$ with $1 \le k < x$, the bound*

$$\pi(x; k, a) = O\left(\frac{x}{\varphi(k) \log(3x/k)}\right)$$

holds.

Let $\mathcal{P}$ be the set of prime numbers. The following estimate can be derived via partial summation from Lemma 3.2, see, for example, the proof of Theorem 3.4 in [22].

Lemma 3.3. *For any integer $f \geq 1$ the bound*

$$\sum_{\substack{p\in\mathcal{P},\, f^2\leq p\leq x\\ p\equiv 1 \pmod f}} \frac{1}{p\log(3x/p)} \ll \frac{\log\log x}{\varphi(f)\log x}$$

holds.

Proof. Let $h = \lfloor 2\log f \rfloor$, $H = \lceil \log x \rceil$. Then

$$\sum_{\substack{p\in\mathcal{P},\, f^2\leq p\leq x\\ p\equiv 1 \pmod f}} \frac{1}{p\log(3x/p)} \leq \sum_{j=h}^{H} \sum_{\substack{p\in\mathcal{P},\, e^j\leq p\leq e^{j+1}\\ p\equiv 1 \pmod f}} \frac{1}{p\log(3x/p)}$$

$$\ll \sum_{j=h}^{H} \frac{1}{e^j \log(3xe^{-j-1})} \cdot \frac{e^j}{\varphi(f)j} \ll \frac{1}{\varphi(f)} \sum_{j=1}^{H} \frac{1}{j\left(\log(3x) - j - 1\right)}.$$

The result now follows. $\square$

3.3 Average multiplicative order

Here we show that the conjecture (5) is wrong and in fact $T_g(L)$ grows faster.

Theorem 3.4. *Under the Extended Riemann Hypothesis, for every integer g which is not a perfect square, there exists a constant $C(g) > 0$ such that*

$$T_g(L) \geq \frac{L}{\log L} \exp\left(C(g)(\log\log\log L)^{3/2}\right).$$

Proof. Let $\mathcal{P}_g$ be the set of $p \in \mathcal{P}$ for which g is a primitive root modulo p. Let us put

$$Q = \exp(\sqrt{\log L}).$$

For an integer $k \geq 2$ we consider the set $\mathcal{L}_g(k, L)$ of positive integers $\ell \in [L/2, L]$ of the form $\ell = p_1 \ldots p_k$ where $p_i \in \mathcal{P}_q$ and $p_i \geq Q$, $i = 1, \ldots, k$.

By Lemma 3.1, considering only those integers $\ell \in \mathcal{L}_g(k, L)$ for which

$p_1, \dots, p_{k-1} \le (L/2Q)^{1/(k-1)}$, and thus $L/2p_1 \dots p_{k-1} \ge Q$, we have

$$
\begin{aligned}
\#\mathcal{L}_g(k, L) &\ge \frac{1}{k!} \sum_{\substack{p_1,\dots,p_{k-1} \in \mathcal{P}_q \\ Q \le p_1,\dots,p_{k-1} \le (L/2Q)^{1/(k-1)}}} \sum_{\substack{p_k \in \mathcal{P}_q \\ L/2p_1\dots p_{k-1} \le p_k \le L/p_1 \dots p_{k-1}}} 1 \\
&= \frac{(A(g)+o(1))L}{2k!} \sum_{\substack{p_1,\dots,p_{k-1} \in \mathcal{P}_q \\ Q \le p_1,\dots,p_{k-1} \le (L/2Q)^{1/(k-1)}}} \frac{1}{p_1 \dots p_{k-1} \log(3L/p_1 \dots p_{k-1})} \\
&\ge \frac{(A(g)+o(1))L}{2k! \log L} \sum_{\substack{p_1,\dots,p_{k-1} \in \mathcal{P}_q \\ Q \le p_1,\dots,p_{k-1} \le (L/2Q)^{1/(k-1)}}} \frac{1}{p_1 \dots p_{k-1}} \\
&= \frac{(A(g)+o(1))L}{2k!} \left(\sum_{\substack{p \in \mathcal{P}_q \\ Q \le p \le (L/2Q)^{1/(k-1)}}} \frac{1}{p} \right)^{k-1}.
\end{aligned}
$$

By partial summation, we derive from Lemma 3.1 that

$$
\sum_{\substack{p \in \mathcal{P}_q \\ Q \le p \le (L/2Q)^{1/(k-1)}}} \frac{1}{p} \sim A(g)(\log\log(L/2Q)^{1/(k-1)} - \log\log Q) \sim \frac{A(g)}{2} \log\log L,
$$

uniformly for k with $\log k = o(\log\log L)$. Therefore, uniformly for k with $\log k = o(\log\log L)$

$$
\#\mathcal{L}_g(k, L) \ge \frac{(A(g)+o(1))^k L(\log\log L)^k}{2^k k! \log L}.
$$

We now denote by $\mathcal{Q}_d(k, L)$ the set of positive integers $\ell \le L$ of the form $\ell = p_1 \dots p_k$ where $p_i \in \mathcal{P}$ are distinct primes, $p_i \ge Q$, $i = 1, \dots, k$, and

$$
\max_{1 \le i < j \le k} \gcd(p_i - 1, p_j - 1) = d.
$$

For $d \le Q^{1/2}$ we use Lemma 3.2 to derive

$$\begin{aligned}
\#\mathcal{Q}_d(k,L) &\le \frac{1}{(k-2)!} \sum_{\substack{p_1,\dots,p_{k-2}\in\mathcal{P}\\ p_1,\dots,p_{k-2}\ge Q}} \sum_{\substack{p\in\mathcal{P}\\ p\ge Q\\ p\equiv 1 \pmod d}} \sum_{\substack{q\in\mathcal{P}\\ Q\le q\le L/pp_1\dots p_{k-2}\\ q\equiv 1 \pmod d}} 1\\
&\ll \frac{L}{(k-2)!\varphi(d)} \sum_{\substack{p_1,\dots,p_{k-2}\in\mathcal{P}\\ p_1,\dots,p_{k-2}\ge Q}}\\
&\qquad \sum_{\substack{p\in\mathcal{P}\\ Q\le p\le L/p_1\dots p_{k-2}\\ p\equiv 1 \pmod d}} \frac{1}{pp_1\dots p_{k-2}\log(3L/pp_1\dots p_{k-2}d)}.
\end{aligned}$$

Applying Lemma 3.3 with $f = d$ (once) and theh $f = 1$ ($k-2$ times), we obtain, that for $d \le Q^{1/2}$

$$\#\mathcal{Q}_d(k,L) \ll \frac{L(\log\log L)^{k-1}}{(k-2)!\varphi(d)^2\log L}.$$

Since $\varphi(d) \gg d/\log\log d$, see Theorem 328 of [40], we conclude that for any $D > 0$,

$$\sum_{Q^{1/2}\ge d>D} \#\mathcal{Q}_d(k,L) \le D^{-1+o(1)}\frac{L(\log\log L)^{k-1}}{(k-2)!\log L}.$$

Also using the trivial bound

$$\#\mathcal{Q}_d(k,L) \ll \sum_{\substack{p_1,p_2\in\mathcal{P},\\ p_1,p_2\le L\\ p_1\equiv p_2\equiv 1 \pmod d}} \frac{L}{p_1p_2} \le L\left(\sum_{\substack{n\le L\\ n\equiv 1 \pmod d}} \frac{1}{n}\right)^2 \ll \frac{L(\log L)^2}{d^2}.$$

for $d > Q^{1/2}$ we derive that

$$\sum_{d>Q^{1/2}} \#\mathcal{Q}_d(k,L) \le Q^{-1/2}L(\log L)^2.$$

Hence, for $D \le Q^{1/2}$

$$\sum_{d>D} \#\mathcal{Q}_d(k,L) \le D^{-1+o(1)}\frac{L(\log\log L)^{k-1}}{(k-2)!\log L}.$$

Finally, let $\mathcal{S}(L)$ be the set of positive integers $\ell \le L$ such that $p^2|\ell$ for some $p \ge Q$. Clearly

$$\#\mathcal{S}(L) \le \sum_{\substack{p\in\mathcal{P}\\ p\ge Q}} \left\lfloor L/p^2 \right\rfloor \ll L/Q.$$

Therefore, for $D_k = 3^k$, for the set

$$\mathcal{R}_g(k,L) = \mathcal{L}_g(k,L) \setminus \left(\bigcup_{d>D_k} \mathcal{Q}_d(k,L) \cup \mathcal{S}(L) \right)$$

we have

$$\#\mathcal{R}_g(k,L) \ge \frac{(A(g)+o(1))^k \, L(\log\log L)^k}{2^k k! \log L},$$

provided $\log k = o(\log\log L)$.

On the other hand, for every $\ell = p_1 \dots p_k \in \mathcal{R}_g(L)$ we have

$$\begin{aligned}
t_g(\ell) &= \operatorname{lcm}(t_g(p_1),\dots,t_g(p_k)) = \operatorname{lcm}(p_1-1,\dots,p_k-1)\\
&\ge \prod_{i=1}^{k}(p_i-1)\prod_{j=1}^{i-1}\frac{1}{\gcd(p_i-1,p_j-1)}\\
&\ge \frac{(p_1-1)\dots(p_k-1)}{D_k^{k^2/2}} \ge \frac{p_1\dots p_k}{2^k D_k^{k^2/2}} \ge \frac{L}{2^{k+1}D_k^{k^2/2}}\\
&\ge \frac{L}{2^{k+1}3^{k^3/2}} \gg \frac{L}{3^{k^3}}.
\end{aligned}$$

Therefore, under the above condition on k, we derive

$$\begin{aligned}
T_g(L) &\ge \frac{1}{L}\sum_{\substack{\ell\in\mathcal{R}_g(k,L)\\ \gcd(g,\ell)=1}}^{L} t_g(\ell) \ge \frac{\#\mathcal{R}_g(k,L)}{3^{k^3}} \ge \frac{(A(g)+o(1))^k \, L(\log\log L)^k}{k!3^{k^3}\log L}\\
&= \frac{L(\log\log L)^k \exp(O(k^3))}{\log L}.
\end{aligned}$$

Taking

$$k = \left\lfloor c(g)\sqrt{\log\log\log L} \right\rfloor$$

for an appropriate constant $c(g) > 0$, depending only on g (which guarantees that the term $(\log\log L)^k$ exceeds, say, the square of factor $\exp(O(k^3))$) we finish the proof. $\square$

As we have remarked, we believe that the bound of Theorem 3.4 is not tight and in fact a stronger bound (6) can be derived by using the method of [57], modified in a similar way as that of [8] to deal only with special primes, see also [25].

It is a very interesting question to obtain more precise information about the behaviour of $T_g(L)$, for example to establish whether (7) is correct. It is possible that the method of [24] combined with the methods and results of [47, 51] are able to handle this task. In fact, even already existing results of [24, 47, 51], without any modifications or adjustments, may shed light on many issues risen by V. I. Arnold in [1, 3, 5, 6].

We also remark that a dual question about the the average value

$$\widetilde{T}(\ell) = \frac{1}{\varphi(\ell)} \sum_{\substack{g=1 \\ \gcd(g,\ell)=1}}^{\ell} t_g(\ell)$$

is studied in [37, 54, 56]. In particular, in [56] one can also find various upper and lower bounds on $\widetilde{T}(\ell)$, while its behaviour on special sequences is considered in [37, 54].

It is well known that if an integer $g > 1$ is fixed then for any function $\varepsilon(x)$ with $\varepsilon(x) \to 0$ as $x \to \infty$, for almost all primes p the bound $t_g(p) \ge p^{1/2+\varepsilon(p)}$ holds, see [23, 26, 44, 65] for various improvements of this result. For almost all integers ℓ, similar type bounds are given in [47].

It is clear that when g varies, $t_g(\ell)$ runs through divisors of $\lambda(\ell)$. In fact through all the divisors of $\lambda(\ell)$. Accordingly the question about the behaviour of $\tau(\lambda(\ell))$ becomes of interest (where $\tau(k)$ is the number of all integer positive divisors of $k \ge 1$). Partially motivated by this relations, F. Luca and C. Pomerance [55] obtained tight bounds on the average value of $\tau(\lambda(\ell))$.

3.4 Average additive order

V. I. Arnold [5] also asks about the average period $Q(\ell)$ of the map $x \mapsto x+a$ in $\mathbb{Z}_\ell$ taken over all $a \in \mathbb{Z}_\ell$. This function, which can be expressed as the following sum over the divisors of ℓ

$$Q(\ell) = \frac{1}{\ell} \sum_{d|\ell} d\varphi(d),$$

has been studied in detail in [37, 54].

In particular, it is shown in Theorem 3.1 of [37] that

$$\frac{1}{L}\sum_{\ell\le L} Q(\ell) = \frac{3\zeta(3)}{\pi^2}L + O\big((\log L)^{2/3}(\log\log L)^{4/3}\big)$$

where $\zeta(s)$ is the *Riemann ζ-function*. This gives a more precise and explicit form of the assertion made in [5] that on average $Q(\ell)$ grows linearly. Clearly, for any prime p, we have $\widetilde{T}(p) = Q(p-1)$, thus it is also interesting to study $Q(\ell)$ on this and some special sequences of ℓ, see [37]. More results on arithmetic properties of $Q(\ell)$ have been established by F. Luca [54].

3.5 Average divisor

We note that well known bounds of number theoretic functions implies that the assertion made in [5] that the "average divisor" of $\varphi(\ell)$ is

$$d(\varphi(\ell)) = \frac{\sigma(\varphi(\ell))}{\tau(\varphi(\ell))} \sim \frac{\ell^\beta}{\log \ell}$$

(where $\sigma(k)$ is the sum of all integer positive divisors of $k \ge 1$) with some $\beta = 0.96 \pm 0.02$ is false. As it follows from the classical number theoretic bounds

$$2 \le \tau(k) \le 2^{(1+o(1))\log k/\log\log k}, \qquad k+1 \le \sigma(k) = O(k\log\log k),$$

see Theorems 317 and 323 of [40], respectively, for any sufficiently large k we have

$$d(k) = \frac{\sigma(k)}{\tau(k)} \sim k^{1+o(1)}.$$

Finally, we mention that the suggestion made in [5] that the average value of $d(k)$ behaves like

$$D(K) = \frac{1}{K}\sum_{k=1}^{K} d(k) \sim \frac{3K}{2\log K}$$

is wrong too. Since $d(k)$ is a multiplicative function, so is $d(k)/k$, which also satisfies the conditions of the *Wirsing theorem*, see [70]. Thus one can easily show that in fact

$$D(K) \sim \kappa\frac{K}{(\log K)^{1/2}}$$

for some absolute constant $\kappa = 0.4067\ldots$, see [10] for this and some other results on the properties of the average divisor, including an asymptotic expansion of $D(K)$. However, the question on the average value of $d(\varphi(\ell))$ is harder and is of ultimate interest.

It can also be relevant to mention that average divisor $d(k)$ takes integer values for almost all integers $k \geq 1$ but is almost never a divisor of k, see [10, 53, 68] and the references therein. Certainly similar questions about $d(\varphi(\ell))$ are very natural and interesting.

4 Repeated squaring and other nonlinear transformations

Using [7, 12, 27, 28, 29, 31] one can also easily derive various uniformity of distribution results for the vectors $\mathbf{a}_{e^m}$ where $e \geq 2$ is a fixed integer. Alternatively, these results can be interpreted as results about orbits of repeated powering $x \mapsto x^e$. In particular, with $e = 2$ one can study the distribution of elements in orbits of repeated squaring $x \mapsto x^2$ in finite fields and rings, see [2, 3] where the corresponding dynamical system is outlined. The results of [27, 28, 29, 31] show that if the orbit is long enough then the vectors $\mathbf{a}_{e^m}$ are uniformly distributed. Using the bound of J. Bourgain [12], one can consider very short orbits (and not necessary fixed values of e) although the bounds obtained within this approach are less explicit.

These results are complemented by the estimates on the orbit lengths of such transformations which are obtained in [30, 58] and which show that these orbit lengths tend to be large (and close to their largest possible values).

The distributional properties of dynamical systems generated by general non-linear transformations $x \mapsto f(x)$ where f is a rational function, over a finite field or a residue ring, have been extensively studied in the literature as well, see [20, 21, 61, 62, 63] and the references therein. As in the case of repeated powering all these results indicate that if the orbit is long enough then its elements are uniformly distributed. On the other hand, these results are still missing their essential counterpart, namely estimates on the orbit length. Obtaining such estimates (for general or specific functions f) is a very important open question.

5 Further remarks and extensions

Results of a different flavour but also describing the distribution of powers of primitive elements modulo a prime p are given in [67].

We have already remarked that analogues of our results hold for an arbitrary ϑ, not necessarily a primitive root, provided the multiplicative order of ϑ is large enough. For more general formulations of Lemma 2.1 and Lemma 2.2, see [33, 35] and [27], respectively.

Analogues of the bound (9) and Lemmas 2.1 and 2.2 are also known for residue rings $\mathbb{Z}_\ell$, see [45, 46, 52] and [28, 29], respectively. Thus one can study orbits of ϑ^m in residue rings as well. In particular, it is well known that one can use these bounds to obtain various uniformity of distribution results suggested in Section 2 of [3].

Furthermore, the dynamical system corresponding to the repeated squaring of a unimodular matrix has been considered in [2]. Using the results and methods of [38], one can prove various uniformity of distribution properties of orbits of such dynamical systems. Accordingly, the results of [7, 41, 50] can be used to obtain similar statements for analogues of the above dynamical systems on elliptic curves over finite fields.

Acknowledgements

The author wishes to thank Florian Luca, Harald Niederreiter, Carl Pomerance, John Roberts and Franco Vivaldi for useful discussions, additional references and encouragement to write this paper. This work was supported in part by ARC grant DP0556431.

References

[1] V. I. Arnold, *Fermat-Euler dynamical systems and the statistics of arithmetics of geometric progressions*, Func. Analysis Appl., **37** (2003), 1–15.

[2] V. I. Arnold, *The topology of algebra: Combinatorics of squaring*, Func. Analysis Appl., **37** (2003), 177–190.

[3] V. I. Arnold, *Topology and statistics of formulae of arithmetics*, Russian Math. Surveys, **58** (2003), 637–664.

[4] V. I. Arnold, *Geometry and dynamics of Galois fields*, Russian Math. Surveys, **59** (2004), 1029–1046.

[5] V. I. Arnold, *Number-theoretic turbulence in Fermat-Euler arithmetics and large Young diagrams geometry statistics*, J. Math. Fluid Mech., **7** (2005), S4–S50.

[6] V. I. Arnold, *Ergodic and arithmetical properties of geometrical progression's dynamics and of its orbits*, Moscow Math. J., **5** (2005).

[7] W. D. Banks, J. B. Friedlander, M. Garaev and I. E. Shparlinski, *Double character sums over elliptic curves and finite fields*, Pure and Appl. Math. Quart., **2** (2006), 179–197.

[8] W. D. Banks, J. B. Friedlander, F. Luca, F. Pappalardi and I. E. Shparlinski, *Coincidences in the values of the Euler and Carmichael functions*, Acta Arith., **122** (2006), 207–234.

[9] W. D. Banks, M. Z. Garaev, F. Luca and I. E. Shparlinski, *Uniform distribution of fractional parts related to pseudoprimes*, Canad. J. Math., (to appear).

[10] P. T. Bateman, P. Erdős, C. Pomerance and E. G. Straus, *The arithmetic mean of the divisors of an integer*, Analytic number theory (Philadelphia, PA, 1980), Lecture Notes in Math., Vol. **899**, Springer, Berlin-New York, 1981, 197–220.

[11] J. Bourgain, *Pointwise ergodic theorems for arithmetic sets*, Inst. Hautes Études Sci. Publ. Math., **69** (1989), 5–45.

[12] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc., **18** (2005), 477–499.

[13] J. Bourgain and M.-C. Chang, *A Gauss sum estimate in arbitrary finite field*, Comptes Rendus Mathematique, **342** (2006), 643–646.

[14] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. Lond. Math. Soc., **73** (2006), 380–398.

[15] J. Bourgain and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, Comptes Rendus Mathematique, **337** (2003), 75–80.

[16] M.-C. Chang, *On a problem of Arnold on uniform distribution*, J. Funcional Analysis, **242** (2007), 272–280.

[17] J. H. H. Chalk, *Polynomial congruences over incomplete residue systems modulo k*, Proc. Kon. Ned. Acad. Wetensch., **A92** (1989), 49–62.

[18] M. Degli Esposti and S. Isola, *Distribution of closed orbits for linear automorphisms of tori*, Nonlinearity, **8** (1995), 827–842.

[19] M. Drmota and R. Tichy, "Sequences, Discrepancies and Applications," Springer-Verlag, Berlin, 1997.

[20] E. D. El-Mahassni, I. E. Shparlinski and A. Winterhof, *Distribution of nonlinear congruential pseudorandom numbers modulo almost squarefree integers*, Monatsh. Math., **148** (2006), 297–307.

[21] E. D. El-Mahassni and A. Winterhof, *On the distribution of nonlinear congruential pseudorandom numbers in residue rings*, Intern. J. Number Theory, **2** (2006), 163–168.

[22] P. Erdős, A. Granville, C. Pomerance and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, Analytic Number Theory, Birkhäuser, Boston, 1990, 165–204.

[23] P. Erdős and R. Murty, *On the order of $a \pmod p$*, Proc. 5th Canadian Number Theory Association Conf., Amer. Math. Soc., 1999, 87–97.

[24] P. Erdős, C. Pomerance and E. Schmutz, *Carmichael's lambda function*, Acta Arith., **58** (1991), 363–385.

[25] K. Ford, *The distribution of totients*, The Ramanujan J., **2** (1998), 67–151.

[26] K. Ford, *The distribution of integers with a divisor in a given interval*, Preprint, 2004.

[27] J. B. Friedlander, J. Hansen and I. E. Shparlinski, *On character sums with exponential functions*, Mathematika, **47** (2000), 75–85.

[28] J. B. Friedlander, J. Hansen and I. E. Shparlinski, *On the distribution of the power generator modulo a prime power*, Proc. DIMACS Workshop on Unusual Applications of Number Theory, 2000, Amer. Math. Soc., 2004, 71–79.

[29] J. B. Friedlander, S. V. Konyagin and I. E. Shparlinski, *Some doubly exponential sums over $\mathbb{Z}_m$*, Acta Arith., **105** (2002), 349–370.

[30] J. B. Friedlander, C. Pomerance and I. E. Shparlinski, *Period of the power generator and small values of Carmichael's function*, Math. Comp., **70** (2001), 1591–1605 (see also **71** (2002), 1803-1806).

[31] J. B. Friedlander and I. E. Shparlinski, *On the distribution of the power generator*, Math. Comp., **70** (2001), 1575–1589.

[32] H. Furstenberg and B. Weiss, *A mean ergodic theorem for $(1/N)\sum_{n=1}^{N} f(T^n x)g(T^{n^2}x)$*, Convergence in Ergodic Theory and Probability (Columbus, OH, 1993), Ohio State Univ. Math. Res. Inst. Publ., 5, de Gruyter, Berlin, 1996, 193–227.

[33] M. Z. Garaev, *Double exponential sums related to Diffie–Hellman distributions*, Int. Math. Res. Notices, **2005:17** (2005), 1005–1014.

[34] M. Z. Garaev, *The large sieve inequality for the exponential sequence $\lambda^{[O(n^{15/14+o(1)})]}$ modulo primes*, Canad. J. Math., (to appear).

[35] M. Z. Garaev and A. A. Karatsuba, *New estimates of double trigonometric sums with exponential functions*, J. Number Theory, **114** (2005), 182–192.

[36] M. Z. Garaev and I. E. Shparlinski, *The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes*, Intern. Math. Res. Notices, **2005:39** (2005) 2391–2408.

[37] J. von zur Gathen, A. Knopfmacher, L.G. Lucht, F. Luca and I. E. Shparlinski, *Average order in cyclic groups*, J. Théorie des Nombres Bordeaux, **16** (2004), 107–123.

[38] D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, *Exponential sums with Dickson polynomials*, Finite Fields and Their Appl., **12** (2006), 16–25.

[39] H. Halberstam and H.-E. Richert, "Sieve Methods," Academic Press, London, 1974.

[40] G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," Oxford Univ. Press, Oxford, 1979.

[41] F. Hess and I. E. Shparlinski, *On the linear complexity and multidimensional distribution of congruential generators over elliptic curves*, Designs, Codes and Cryptography, **35** (2005), 111–117.

[42] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math., **225** (1967), 209–220.

[43] M. N. Huxley, *A note on polynomial congruences*, Recent Progress in Analytic Number Theory, Vol.1, Academic Press, 1981, 193–196.

[44] H.-K. Indlekofer and N. M. Timofeev, *Divisors of shifted primes*, Publ. Math. Debrecen, **60** (2002), 307–345.

[45] S. V. Konyagin and I. E. Shparlinski, "Character Sums with Exponential Functions and Their Applications," Cambridge Univ. Press, Cambridge, 1999.

[46] N. M. Korobov, *On the distribution of digits in periodic fractions*, Mat. USSR-Sb., **18** (1972), 659–676.

[47] P. Kurlberg and C. Pomerance, *On the period of the linear congruential and power generators*, Acta Arith., **119** (2005), 149–169.

[48] P. Kurlberg and Z. Rudnick, *On the distribution of matrix elements for the quantum cat map*, Annals of Math., **161** (2005), 489–507.

[49] M. Laczkovich,*Discrepancy estimates for sets with small boundary*, Studia Sci. Math. Hungar., **30** (1995), 105–109.

[50] T. Lange and I. E. Shparlinski, *Certain exponential sums and random walks on elliptic curves*, Canad. J. Math., **57** (2005), 338–350.

[51] S. Li and C. Pomerance, *On generalizing Artin's conjecture on primitive roots to composite moduli*, J. Reine Angew. Math., **556** (2003), 205–224.

[52] R. Lidl and H. Niederreiter, "Finite Fields," Cambridge University Press, Cambridge, 1997.

[53] F. Luca, *On $f(n)$ modulo $\omega(n)$ and $\Omega(n)$ when f is a polynomial*, J. Austral. Math. Soc., **77** (2004), 149–164.

[54] F. Luca, *Some mean values related to average multiplicative orders of elements in finite fields*, Ramanujan J. of Math., **9** (2005), 33–44.

[55] F. Luca and C. Pomerance, *On the average number of divisors of the Euler function*, Publ. Math. Debrecen., (to appear).

[56] F. Luca and I. E. Shparlinski, *Average multiplicative orders of elements modulo n*, Acta Arith., **109** (2003), 387–411.

[57] H. Maier and C. Pomerance, *On the number of distinct values of Euler's ϕ function*, Acta Arith., **49** (1988), 263–275.

[58] G. Martin and C. Pomerance, *The iterated Carmichael λ-function and the number of cycles of the power generator*, Acta Arith., **118** (2005), 305–335.

[59] H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc., **84** (1978), 957–1041.

[60] H. Niederreiter, "Random Number Generation and Quasi–Monte Carlo Methods," SIAM Press, 1992.

[61] H. Niederreiter, *Design and analysis of nonlinear pseudorandom number generators*, Monte Carlo Simulation, A.A. Balkema Publishers, Rotterdam, 2001, 3–9.

[62] H. Niederreiter and I. E. Shparlinski, *Dynamical systems generated by rational functions*, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **2643** (2003), 6–17.

[63] H. Niederreiter and A. Winterhof, *Exponential sums for nonlinear recurring sequences*, Finite Fields and Their Appl., (to appear).

[64] H. Niederreiter and J. M. Wills, *Diskrepanz und Distanz von Massen bezuglich konvexer und Jordanscher Mengen*, Math. Zeitschrift, **144** (1975), 125–134.

[65] F. Pappalardi, *On the order of finitely generated subgroups of* $\mathbb{Q}^*$ (mod p) *and divisors of* $p-1$, J. Number Theory, **57** (1996), 207–222.

[66] A. G. Postnikov, "Ergodic Problems in the Theory of Congruences and of Diophantine Approximations," Amer. Math. Soc., 1967.

[67] Z. Rudnick and A. Zaharescu, *The distribution of spacings between small powers of a primitive root*, Israel J. of Math., **120** (2000), 271–287.

[68] C. Spiro, *How often is the number of divisors of* n *a divisor of* n*?*, J. Number Theory., **21** (1985), 81–100.

[69] H. Weyl, *On the volume of tubes*, Amer. J. Math., **61** (1939), 461–472.

[70] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen*, Math. Ann., **143** (1961), 75–102.